TDC

Theater Deployable Communications

Baseline Requirements Document

Network Control Center Deployed - Heavy Module
(v3)
Nov 2003

ESC/NI4T
5 Eglin Street
Hanscom AFB, MA 01731

Table of Contents

List of Tables

List of Figures

1.0 SCOPE

This requirements document establishes the performance, manufacture and test requirements for the TDC Network Control Center-Deployed Heavy Module v3.

2.0 APPLICABLE DOCUMENTS

To the extent specified herein, the following documents of latest current issue on the date of this Baseline Requirements Document form part of this BRD.

Table 1 - Standards and Applicable Documents

Document Number	Title
	USAF Server Naming Conventions
	TDC NCC-D Naming List, IP Assignments, and Passwords
	NCC-D Software Installation Manual V2.0
	DoD Symantec Host File
	TDC Standards Document

3.0 REQUIREMENTS

The purpose of the NCC-D is to allow the deployed communications personnel to proactively and reactively manage and protect the network infrastructure, and to protect sensitive data transported over the WAN via state-of-the-art COTS products that will satisfy the Air Force's need for standardization and reduced life cycle costs.

The Heavy NCC-D package has been defined to support a deployed unit with up to 1,200 personnel and accomplish the goals stated above.

The Heavy NCC-D package can be deployed on a NIPRNET side or SIPRNET side with minor software configuration differences such as naming conventions reflected in this BRD.

3.1 Package Definition

A Heavy NCC-D package contains both modules and the monitor kit. The Heavy NCC-D Package V3.0 shall be integrated and configured to the network architecture depicted in Figure 1. The Heavy NCC-D Package V3.0 shall provide maximum commonality with the existing TDC equipment and be compatible with the previous NCC-D builds. The number of different configurations within the NCC-D suite itself shall be minimized. The Heavy NCC-D Package V3.0 for SIPRNET and Heavy NCC-D Package V3.0 for NIPRNET are identical, with the exception of naming conventions, unlike the previous builds.

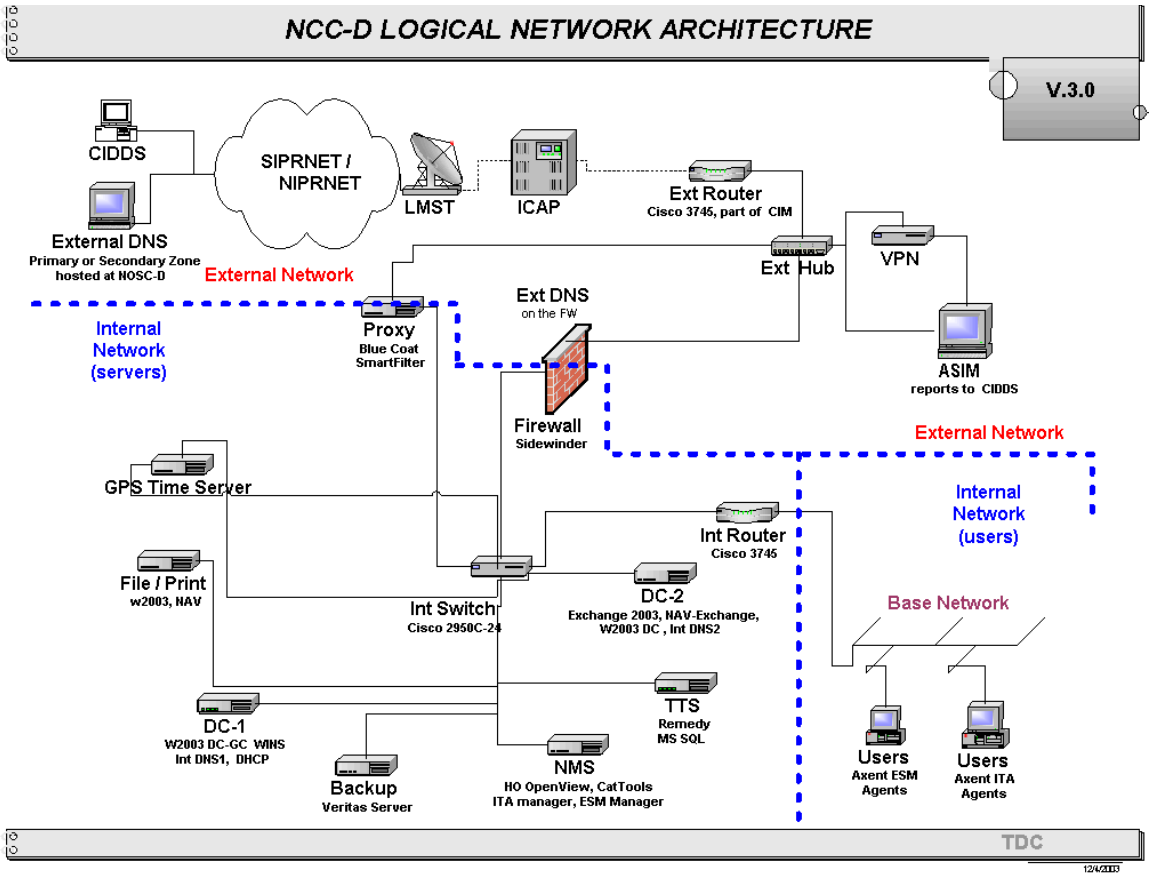

Figure 1 - NCC-D Version 3.0 Logical Network Architecture

3.2 Performance Requirements

Figure 2, Notional Heavy NCC-D Package Configuration, is provided as a reference to clarify the specific Heavy NCC-D Package requirements.

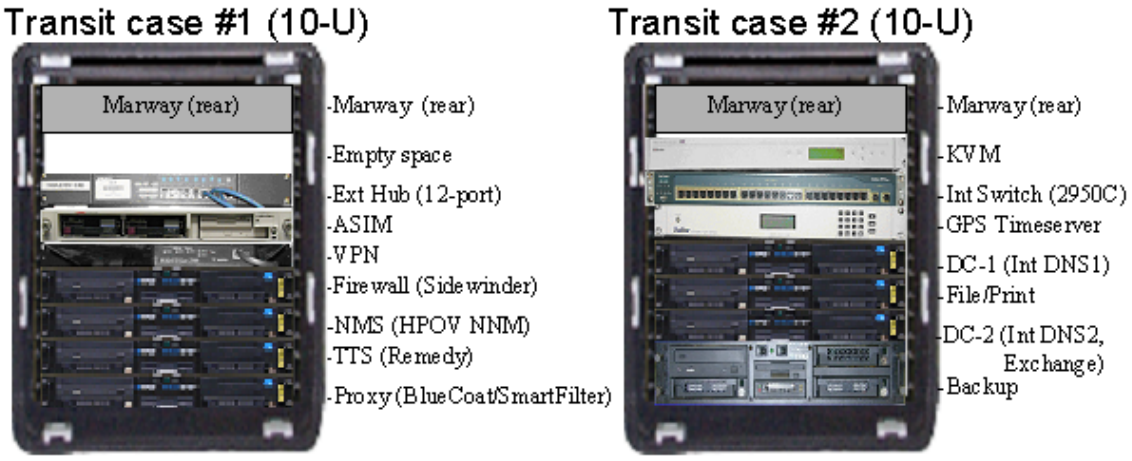

Figure 2 - Notional Heavy NCC-D Package Configuration

3.2.1 Software Requirements

Note: Software versions listed in this section are subject to change as the latest versions of the software are released and approved by the TDC program office.

Table 2 - NCC-D Software Versions and Sources

Software	Source
Sidewinder V5.2.1.7	CFE
Blue Coat Security Gateway Version 2.1.94	CFE
SmartFilter Version 3.0	CFE
HP OpenView Network Node Manager (NNM) V7.x	CFE
Kiwi CatTools V2.0.4	GFE (AF Enterprise License)
Remedy V5.1.2	GFE (AF Enterprise License)
MS SQL Server 2000 Std Edition English w/ 10 CAL	CFE
Perl V5.0	GFE
TDC Remedy schema	GFE
DNS / WINS / DHCP/ IIS/ IE Windows 2003 based Version determined by OS	Included on Win 2003 CD
MS Exchange 2003 Enterprise Edition with 25 client licenses	CFE
Microsoft Outlook 2000 / 2002 / 2003	Included with Exchange
Veritas Backup Exec Version 9.1 Server, Exchange Client, MS SQL Client, 5 Remote Open File Clients	CFE
Symantec ESM Version 6.0	GFE (AF Enterprise License)

Table 2 - NCC-D Software Versions and Sources

Software	Source
Symantec HIDS v 4.1	GFE (AF Enterprise License)
Symantec Anti-Virus Corporate Edition Version 8.1	GFE (AF Enterprise License)
Symantec Mail Security Version 4.0	GFE (AF Enterprise License)
Windows 2003 Server	CFE
The latest Service packs and Security Fixes	Approved by TDC program office
Time Server clients for Windows 2003	CFE
Password Policy Enforcer (PPE) v3.6	GFE
Adobe Acrobat Reader	GFE

GFE=Government Furnished Equipment
CFE=Contractor Furnished Equipment

All software packages shall include the media kits, one per each package installed.

The contractor shall provide software images and appropriate scripts to automate the reloading of all Windows-based servers to include applications. These images shall provide the capability to choose (change) the system NetBIOS name, System Fully Qualified Domain Name (FQDN) (DNS name), IP address, and the system SID (Microsoft Security Identifier). This will speed up frequent re-installations of all NCC-D servers in the field and reduce the amount of time needed for deployment. The contractor shall provide one CD with the software image for each server type for each package. The contractor shall choose and acquire all the appropriate tools for this task.

Table 3 identifies the software to be installed on each server.

Table 3 - Server Software Installation Matrix

Software	DC1 (Domain Control-ler)	DC2 (Domain Control-ler)	FW (Fire-wall)	Proxy	TTS (Trouble Ticket-ing System)	NMS (Network Manage-ment Server)	File/ Print	Backup
W2003 server	X	X			X	X	X	X
DC	X	X						
AD GC	X							
Sidewinder			X					
BlueCoat Security Gateway				X				
SmartFilter				X				
WINS	X							
DHCP	X							
SNMP service	X	X	X	X	X	X	X	X
MS IIS		X						
PPE	X							

Table 3 - Server Software Installation Matrix

Software	DC1 (Domain Control-ler)	DC2 (Domain Control-ler)	FW (Fire-wall)	Proxy	TTS (Trouble Ticket-ing System)	NMS (Network Manage-ment Server)	File/ Print	Backup
Int DNS	X	X	X					
Ext DNS			X					
Internet Explorer	X	X			X	X	X	X
Outlook 2002 Client		X			X			
Exchange 2003 Server Enterprise		X						
SQL Server 2000 + SP3					X			
SQL Scripts					X			
Remedy ARSPerl					X			
Perl					X	X		
Remedy ARSPerl					X	X		
HPOV NNM Enterprise						X		
Perl Scripts					X	X		
CatTools						X		
Symantec AntiVirus Corp. Ed.							X	
Symantec AntiVirus Client	X	X			X	X	X	X
Symantec Mail Security		X						
Symantec HIDS/ESM Managers						X		
Symantec HIDS/ESM Agent	X	X			X	X	X	X
Time Serv (clients)	X							
Veritas Server Software								X
Veritas for Exchange with Open File Option		X						
Veritas for MS SQL with Open File Option					X			
Adobe Acrobat Reader	X	X			X	X	X	X
Veritas Agent with Open File Option	X					X	X	X

3.2.1.1 General Requirements

Operating System. The operating system for the NCC-D V3.0 build shall be Windows 2003 server; this requirement is not applicable to the Sidewinder firewall and appliances (Timeserver and the Proxy). All the server hard drives shall be partitioned using the NTFS file system. Each hard drive shall be partitioned with two (2) partitions in order to meet security requirements of the USAF. The amount of space on each partition shall be carefully calculated for each individual server depending on application / functionality.

Active Directory (AD) shall be installed as a main tool to manage objects and security in the NCC-D suite of applications. Initial installation of NCC-D AD shall be confined to inside the NCC-D security perimeter.

The baseline Schema for Active Directory shall be the default (out of the box) schema plus the Exchange 2003 extensions: Custom Attributes.

Passwords. The contractor shall install the software using the default set of passwords provided by the Government in the NCC-D Naming List, IP Assignments, and Passwords document. A sheet listing these default passwords shall be included with each delivered equipment suite so that each receiving unit can operate the software.

SNMP Management. All servers, etc. in the NCC-D suite shall be SNMP enabled, and traps from them and from other networking gear shall be sent to the NMS Server. The Internal and External Routers and the Internal Switch also need SNMP configuration.

Backup. Exchange and MS SQL servers shall have special server agents (see Exchange and SQL sections) being able to backup the specific database open files. All the rest of the servers shall have remote agents with open file backup option.

3.2.1.1.1 Specific Server Requirements

3.2.1.1.2 Domain Controller (DC)-1 Server Software

The contractor shall install the software on the DC-1 server in accordance with Table 3.

All servers on the internal burb of the firewall shall be installed as part of Microsoft Active Directory (AD). The main installation of AD is to be performed on two Domain Controllers.

The First Domain Controller (DC-1) will become a GC (Global Catalog) and shall also have DNS and WINS servers installed. All the W2K administration tools including Schema Editing shall be installed.

DNS. Internal DNS server shall be installed on the first DC. Internal DNS server shall be AD-enabled for all Windows machines and at the same time be able to support internal UNIX machines. All DNS queries to the outside world shall go to the internal burb of the firewall and further to the external DNS. No DNS queries from the client machines shall go directly to the outside world, only through the Internal DNS. Since Active Directory domains must correlate to valid DNS namespace, the recommended naming conventions for DNS are the same as the domain naming conventions for AD.

WINS. WINS server shall be installed on the first DC for backwards compatibility with legacy / NT servers and to support NetBIOS names.

DHCP. DHCP server shall be installed on the DC-1 server, but the service shall be disabled.

IIS. Do not install Internet Information Server (IIS) on the first DC.

For initial pre-deployment installation Internal Domain Name Service (DNS) shall be setup as a dual master AD-enabled DNS. Both DNS servers shall be installed on top of Domain Controllers.

3.2.1.1.3 Domain Controller (DC)-2 Server Software

The contractor shall install the software on the DC-2 server in accordance with Table 3. The DC-2 server (second Domain controller) shall have IIS, Exchange 2003 server and a second primary master DNS.

The Exchange 2003 organization shall be named "ORGANIZATION" according to AF standards. Warning: this name cannot be changed without reinstalling all Exchange servers in the forest. The sample GAL, provided as GFE, shall be moved into Active Directory. This GAL shall be inputted in AD as Contacts, not Users. See the USAF Naming Conventions document for more information on naming conventions.

Address lists shall be organized as a hierarchy of nested address lists and empty address lists. A nested address list is an address list located under another address list. An empty address list is used as a node, which contains other address lists and does not have a membership because it was created without filter rules.

USAF-specific Site Attributes / Extension Attributes (former Custom Attributes):

Custom Attribute 1	Rank
Custom Attribute 2	MAJCOM
Custom Attribute 3	Unique ID

Two Symantec AntiVirus programs shall be installed on the DC-2 Server.

- Symantec AntiVirus Corporate Edition Client has to be pushed to the DC-2 Server
- Symantec AntiVirus for Microsoft Exchange Server has to be installed on the DC-2 Server. This program will require a separate license and needs to be installed only on the DC-2 machine itself.

When configuring Microsoft Exchange, an SMTP connector or SMTP virtual server must be configured to forward messages to the internal burb of the firewall instead of accepting the default configuration (Forward all messages to host and enter the IP address of the firewall's internal burb). The contractor shall also configure the SMTP virtual server to only relay messages for authenticated users (default).

3.2.1.1.4 Firewall Server Software

The contractor shall install the software on the Firewall server in accordance with Table 3. The third DNS server shall be installed as a part of the Firewall functionality and will be a slave DNS.

The firewall software shall be installed with the following configurations:

Burb 1 shall be the internal burb, named “Internal”, and burb 2 shall be the external burb, named “External”.

The “default route” IP address shall be the IP address of the External Router.

Secure Split DNS – The internal side of the firewall shall be a slave DNS server to the primary internal DNS server. On the external side an External DNS server shall be set up as master on the external side for initial installation. In addition, the contractor shall write the procedures detailing the installation and configuration of the external side of the firewall as a slave DNS.

HTTP protocol shall not be allowed to / from the firewall as it shall be going to the Proxy. Proxies to be allowed: DNS, PING out from the internal network; TELNET out from the internal network; SNMP from the internal burb only to the External router; Remedy DSO, SMTP.

Sendmail Server Configuration shall be selected as the Secure split SMTP server option. The SMTP proxy shall be disabled. The Sendmail server shall be enabled on both the internal and external burbs. The firewall shall be configured to perform header stripping so as not to advertise the IP address and fully qualified domain name of the Exchange server.

SNMP Configuration – The firewall shall not allow SNMP into the network from the external burb, except for communication between the external router and the NMS server.

3.2.1.1.5 Proxy Server Software

The contractor shall install the software on the Proxy server in accordance with Table 3. The Web Proxy Server for the NCC-D V3.0 build is Blue Coat Security Gateway. Web Content Filtering SmartFilter shall be installed on the same machine.

The Proxy server shall be installed in such a way so that web traffic will bypass the Sidewinder firewall and be handled by Blue Coat only. Proxy and administrative ports shall be chosen from an unpredictable range (not from 8080 – 8087 range or port 80). All e-mail and other references to bluecoat.com shall be removed. All Inbound Connections must be rejected by the external side of the proxy. The default gateway for the external interface of the proxy shall be the external router. The proxy server shall be configured with settings that optimize operation with an external link with low bandwidth.

3.2.1.1.6 Trouble Ticketing System Software

The contractor shall install the software on the TTS server in accordance with Table 3. The Trouble Ticketing System (TTS) uses two servers, Remedy as the front end and MS SQL as the back end, installed on the same machine. The contractor shall install/configure SQL backup scripts on the TTS server. In addition, TDC Remedy schema shall be installed on the TTS server.

E-mail options of Remedy shall be installed and configured. The Remedy server shall be able to communicate with the NMS server to allow the automatic creation of trouble tickets resulting from critical nodes going down in HP OpenView Network Node Manager.

3.2.1.1.7 Network Management Server Software

The contractor shall install the software on the NMS server in accordance with Table 3. During installation of HP OpenView Network Node Manager, the contractor shall include the loading of the vendor MIBs. The NMS server shall be able to communicate with the Remedy server to allow it to automatically create trouble tickets as a result of critical nodes going down in HPOV NNM.

3.2.1.1.8 File & Print Server Software

The contractor shall install the software on the File & Print server in accordance with Table 3.

Symantec Anti Virus Corporate addition Server shall be installed on the File and Print Server and configured to distribute NAV client software and virus definitions updates to the rest of the servers and workstations in the domain. The virus definition shall be configured to download from a DoD approved web site, not from the Symantec Internet site, in accordance with the DoD Symantec host file provided by the Government.

Symantec Anti Virus Client installations shall be pushed to the servers and workstations on the internal burb.

The following configurations shall be established:

- Auto Protect options: Repair infected attachment and deliver; Delete infected attachment
- Global Options: Type email of recipients of email notifications; No LiveUpdate

3.2.1.1.9 Backup Server Software

The contractor shall install the software on the Backup server in accordance with Table 3.

The backup server software shall be installed on a special backup server capable of backing up the all NCC-D servers as needed. An operational backup will be performed on the hard drives of the backup server and archiving can be done on the tape. Exchange and MS SQL servers shall have special server agents (see Exchange and SQL sections) being able to backup the specific database open files. All the rest of the servers shall have remote agents with open file backup option.

Each server in the NCC-D suite will be fully backed-up once per week and incrementally backed-up daily; this practice needs to be configured and reflected in the documentation/manuals.

3.2.2 Hardware Requirements

The contractor shall provide all required hardware except the ASIM server and associated VPN.

3.2.2.1 General Server Requirements

All servers shall be rack mountable in a standard TDC transit case. All the servers shall have the ability to slide in mounting brackets.

- Size. Servers shall minimize size and weight and provide adequate space for all the internal component to avoid external peripherals. The recommended size configuration for all servers is 1U, unless specified otherwise.

- Hard Drives. Hard Drives shall be externally removable storage to be compliant with security requirements associated with classified operations. Hard drives shall be configured with hardware RAID 1 (mirror). Each hard drive capacity shall be at least 140 GB to ensure application requirements are met. All server hard drives shall have a Small Computer System Interface (SCSI) interface.

- Memory. At least 4 GB of memory (RAM) shall be provided to support the server's applications with acceptable performance while under full load conditions, unless specified otherwise. The memory shall be provided in at least two (2) units (modules, chips) for redundancy.

- Processors and motherboards. Multi-processor servers are an acceptable method of fulfilling performance requirements. All processors and motherboards shall be certified by manufacturer as SERVER class processors and motherboards. Processors shall be Intel-based to ensure full compatibility with any server software being used by NCC-D (check Intel web site for the processors approved for server use).

- Server Peripherals. All servers shall have Floppy and CD-RW/DVD Combo drives (Combo is acceptable). Video, dual 10/100/1000 NIC card and a SCSI card shall be integrated or on separate cards.

3.2.2.2 Specific Server Requirements by Function

- Firewall. The Firewall hardware shall be Sidewinder certified (Secure Computing) out of the box for Sidewinder Version 5.2.1 and above. The server shall provide two 10/100 BaseT NIC Ethernet interfaces to provision the external and internal connections of the firewall. Firewall memory (RAM) shall be 2GB according to Sidewinder recommendations (maximum supported memory for the best performance).

- Proxy. The NCC-D proxy for NCC-D V3.0 shall be a BlueCoat SG800 1U appliance with a minimum of 2 hard drives of 72 GB each and 1.5 GB of memory.

- Backup Server. The backup server shall provide maximum possible hard drive space for operational backups of server hard drives. To achieve this result the backup server is recommended to be no more than a 2U server with at least 4 (four) hard drives. The hard drives shall be the same hard drives as in all other servers to minimize sparing requirements. The backup server shall have a built-in backup media of at least 100 GB

uncompressed capacity for normal archiving of NCC-D data in order to be compatible with the amount of data backed up for archiving. A minimum of 2 GB of memory is acceptable in this server according to software specifications.

3.2.2.3 Keyboard/Mouse/Monitor

Each NCC-D package shall have three Keyboard/Mouse/Monitor sets. All of them shall fit into one standard TDC Monitor Transport Kit.

Keyboards and mice shall be PS-2. Optical mice shall be provided.

Monitors shall be at least 1024 x 768 and 256 colors compatible.

All of the above shall be W2K compatible.

3.2.2.4 KVM Switch

The KVM switch shall provide at least 10 (ten) server ports and 3 (three) user ports, and be able to cascade for expansion /scalability. The KVM shall provide an on-screen interface controlled by the keyboard for each user. The KVM must be capable of providing different levels of login based on authorization / authentication.

3.2.2.5 Ethernet Switch / Hub

The Ethernet switch shall have 24 (twenty four) 10/100 BaseT ports and 2 (two) 100 BaseSX ports and shall be terminated at the Signal Entry Panel (SEP) with ST type connections. The Ethernet switch shall be compatible with existing TDC capabilities concerning v-LAN and clustering solutions.

The hub shall have a minimum of 8 (eight) 10/100 BaseT ports.

3.2.2.6 Timeserver

The timeserver shall be GPS capable and be able to provide network time services to IP-based clients (servers, routers, switches, etc.). A lightning arrestor shall be installed between the GPS timeserver and antenna. The timeserver shall have an internal high stability oscillator to provide a fallback capability in case of loss of GPS signal.

3.2.2.7 Signal Entry Panel

The contractor shall provide a Signal Entry Panel (SEP) for each transit case to facilitate connectivity for all hard-to-reach hardware connections in the NCC-D package, such as KVM connections, console port connections, etc.

For reference purposes, the SEP from the previous NCC-D build is provided here:

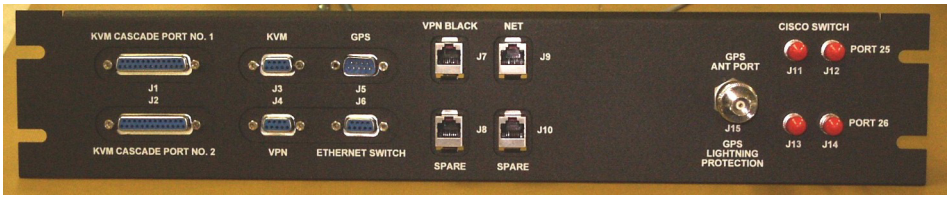

Figure 3 - NCC-D Version 2 Signal Entry Panel

3.2.2.8 ASIM and VPN Hardware

The ASIM server is Compaq DL360 1U Server, and the VPN box is Alcatel 2500 Permit. The contractor is not required to provide or install ASIM and its associated VPN. The contractor shall provide sufficient space (2U) for the installation of ASIM and VPN. The contractor shall provide additional connectivity for this hardware: four (4) RJ-45 connectors and one DB-9 connector on the SEP and two (2) switched power outlets. Additional power receptacles shall be provided to accommodate the above hardware. Heat consumption shall be designed with this hardware in mind.

3.2.3 Electrical Interfaces (External)

The NCC-D package shall be internally wired to provide all the required connections, except the input power.

The input power connection shall be at the power distribution unit (recommended solution is Marway power conditioner for consistency with TDC-ICAP).

3.2.3.1 Prime Power

The NCC-D Packages shall be designed to operate from 100 to 127 VAC and 200 to 240 VAC, 50 to 60 Hz, single-phase, three-wire power. The maximum current shall not exceed 20 amperes at 120 VAC or 10 amperes at 230 VAC. The NCC-D Package shall include an internal power distribution unit to minimize line transients and EMI. The prime power connector shall be an IEC 320-C20 receptacle (“PC power cable”).

3.2.3.2 IP 10BaseT/100BaseTX/1000BaseTX

See TDC Standards Document

3.2.3.3 100BaseFX

See TDC Standards Document

3.2.3.4 Console Ports (DB9, RS-232)

See TDC Standards Document

3.2.4 Electrical Interfaces (Internal) - TBS

The contractor shall provide documentation that will show the internal wiring of the major Package components and the details of each major cable assembly internal to each case.

3.2.5 Packaging/Transit Cases and Monitor Kits

All NCC-D equipment shall be packaged into transit cases and monitor kits in accordance with the TDC Standards Document.

3.2.5.1 Weight

Each transit case, including all internally carried cables, shall not exceed the weight requirement contained in the TDC Standards Document. In addition, each case shall be a 3-person transportable container.

Each monitor kit, including all internally carried items, shall not exceed the weight requirement contained in the TDC Standards Document. In addition, each kit shall be a 2-person transportable container.

3.2.5.2 Storage Space

The storage space shall be in accordance with the TDC Standards Document.

3.2.6 Cables and Accessories

All cables in the NCC-D suite shall be of appropriate length.

Network Ethernet cables shall be Cat. 5 cables. Network cables shall be color-coded (Red for External, Blue for Internal side of the firewall).

Applicable cables for the servers shall be connected to a KVM switch.

All cables shall be secured with a non-conductive adhesive to insure inadvertent removal and shall also be routed and secured to further insure inadvertent removal. *Note:* This adhesive shall also be easily removable.

3.2.7 Marking & Labeling

All NCC-D equipment shall be marked and labeled in accordance with the TDC Standards Document. NCC-monitor kits shall be marked according to the requirements for NCC-D modules (vice kits).

In addition, NIC ports are to be color coded with paint to match cables. Etching and/or other permanent marking system shall be used for marking cables. Marking shall be easily readable on the cables.

3.2.8 Reliability

TDC NCC-D equipment shall operate reliably in a military environment. The lifetime of each server and its components as well as service levels shall comply with the best industry standards.

The NCC-D components have a Mean Time Between Failure (MTBF) commensurate with similar commercial equipment in its class. The actual MTBF for the major system components shall be supplied **TBS**. Where reliability data is not readily available from the vendor, this shall be indicated.

3.2.9 Maintainability

Maintainability characteristics will be part of the selection criteria for all hardware. Ease of maintenance, such as accessibility to Line Replaceable Units, fault detection/isolation software capability, and fault annunciation shall be considered.

3.2.10 Environmental Conditions

3.2.10.1 Temperature

During storage, transport and operation the package shall withstand exposure to Operating temperatures of 0 – 120 degrees F and Non-Operating temperatures of 0 – 160 degrees F. Relative humidity characteristics for the major equipment components shall provide normal operation at or below 95% humidity.

3.2.10.2 Altitude

Altitude characteristics for the major equipment components shall provide normal operation at or below 8000 ft and non-operating of up to 40,000 ft.

3.2.10.3 Sand and Dust

During storage and transport, the package is protected when exposed to sand and dust in accordance with the best commercial practices for close proximity to operating aircraft. During operation with the covers removed, the Package shall withstand sand and dust in accordance with the best commercial practices for natural conditions.

3.2.10.3.1 Shock

The package equipment rack shall be equipped with rubber shock isolation mounts and shall be protected from shocks induced during handling, setup and teardown. Packages and components shall operate without degradation following exposure to the non-operating shock environment described by Method 516.4, Procedure VI (Bench Handling) of MIL STD 810E.

3.2.10.4 Vibration

The package shall be equipped with rubber shock isolation mounts so that the Package can withstand the vibration encountered while being transported by commercial and military airlift, sealift and vehicular (over unimproved roads) systems

3.3 Design and Construction

3.3.1 Material Parts and Processes

The package shall be built to good commercial practices. Mechanical and electrical interchangeability shall exist between like systems, subsystems, assemblies, and subassemblies and shall consist of replaceable parts.

3.3.2 Safety

The NCC-D equipment shall not present any safety, fire or health hazard to personnel.

3.3.2.1 Electrical Safety

The Heavy NCC-D package shall be designed to eliminate the hazard to personnel of inadvertent lethal voltage contact. All electrical conductors carrying voltages in excess of 70 volts shall be insulated to prevent contact or covered by a protective barrier. All removable protective barriers shall be interlocked to automatically disconnect power behind the barrier upon removal or clearly marked with a warning label that indicates the voltage potential that will be encountered behind the barrier. All warning labels shall be visible after the cover has been removed.

3.3.2.2 Mechanical Safety

All sharp surfaces shall have protective covers or other suitable features to minimize injury where personnel are likely to be exposed to such surfaces.

3.4 Logistics

The Package accommodates a two level maintenance concept: organizational (Air Force personnel) and depot (contractor personnel). Removal and replacement of an LRU is defined at the organizational level and any needed repair of the LRU is defined at the depot level. Any special test or support equipment required to effect removal or replacement of an LRU at the organizational level shall be provided as part of the module. No more than two persons shall be required to remove or replace an LRU. An LRU is defined as the lowest element of the Package, which can be isolated to be faulty through inspection, built-in test, technical manuals, TDC NCC-D system performance, spares substitution or other diagnostic aid approved by the Government for organizational level maintenance. This is exclusive of expendables such as fuses, lamps and LEDs.

4.0 QUALITY ASSURANCE PROVISIONS

4.1 General

The quality assurance program includes tests and other evaluations to the extent specified herein. The quality assurance program is designed to verify the electrical, mechanical and functional characteristics of each module. The purpose is to ensure that each module complies with or performs better than the requirements specified herein.

4.2 Responsibility for Inspection

Unless otherwise specified in the contract, the contractor shall be responsible for the performance of all inspection requirements and may use his own or any other facilities suitable for the performance of the inspection requirements. The Government reserves the right to perform any of the inspections set forth in the specification where such inspections are deemed necessary to assure supplies and services conform to the prescribed requirements.

4.3 Product Qualification Test (PQT)

Inspections, analyses, demonstrations and tests verify compliance of Section 3 of this specification on the first production unit.

4.4 Production Acceptance Test (PAT)

Each module delivered to the Government undergoes an Acceptance Test Process as identified in Table 4. The acceptance test verifies that the module interfaces are operating properly prior to delivery to the Government.

4.5 Verification Cross Reference Matrix (VCRM)

Table 4 provides a list of each Section 3 requirement and the verification method to be used. The following paragraphs define the codes employed in the VCRM. Unless otherwise noted, where more than more one verification method is shown, one method or a combination of methods may be used to show compliance.

4.5.1 Not Required (N/R)

This method indicates that verification is not required because the paragraph is a title, heading, general introductory paragraph or statement of a goal and contains no “shall” or “must” statements.

4.5.2 Inspection

Inspection is a method of verification of the module performance or characteristics by examination of the equipment or associated documentation. Inspections are conducted with the use of inspection tools, measurement devices, visual means and comparison. Most inspections apply to verification of requirements associated with physical characteristics such as size, weight,

appearance, adherence to specified standards and engineering practices, quality design, and construction supported with quality documentation. Inspections also include the auditing of manufacturer's data that verifies the performance of non-developmental items that comprise the TDC ICAP module. Inspections may occur during any assembly stage of the unit under test.

4.5.3 Analysis

Analysis is a method of verification through technical evaluation of calculations, computations, models, analytical solutions, use of studies, reduced data, and/or representative data to determine that the item conforms to the specified requirements.

4.5.4 Demonstration

Demonstration is a method of verification whereby the properties, characteristics and parameters of the item are determined by observation alone and without the use of instrumentation for quantitative measurements. This method is used when a requirement does not contain a specific numerical parameter that must be measured. Demonstrations may occur during verification of a unit under test at any assembly stage. Pass/fail criteria are simple yes/no indications of functional performance since no quantitative values are specified.

4.5.5 Test

Test is a method to verify that a specified requirement is met by thoroughly exercising the applicable item under specified conditions and by using the appropriate instrumentation in accordance with test procedures. This method requires the use of laboratory equipment, simulators, or services to verify compliance to the specified requirements. This method is used when it is practicable to make direct or indirect measurement of a specified numerical parameter to verify compliance with a requirement. Tests may occur during verification of a unit at any assembly stage. Actual measured values are recorded, and pass/fail is determined by comparing the measured value with the specified value. Measurement accuracy is precise enough to ensure that the measured value is within the specified tolerance.

Table 4 - Verification Cross Reference Matrix

		Verification Method					
			PQT				
Paragraph	Title	N/R	Inspect	Analysis	Demo	Test	ATP
3.	REQUIREMENTS	X					
3.1	Package Definition			X			
3.2	Performance Requirements	X					
3.2.1	Software Requirements		X		X		X
3.2.1.1	General Requirements		X	X	X		X
3.2.1.2	Specific Server Requirements	X					
3.2.1.2.1	Domain Controller (DC)-1 Server Software				X		X

Table 4 - Verification Cross Reference Matrix

Paragraph	Title	Verification Method					
			PQT				
		N/R	Inspect	Analysis	Demo	Test	ATP
3.2.1.2.2	Domain Controller (DC)-2 Server Software				X		X
3.2.1.2.3	Firewall Server Software				X		X
3.2.1.2.4	Proxy Server Software				X		X
3.2.1.2.5	Trouble Ticketing Server Software				X		X
3.2.1.2.6	Network Management Server Software				X		X
3.2.1.2.7	File & Print Server Software				X		X
3.2.1.2.8	Backup Server Software				X		X
3.2.2	Hardware Requirements		X				
3.2.2.1	General Server Requirements		X				X
3.2.2.2	Specific Server Requirements by Function		X				X
3.2.2.3	Keyboard/Mouse/Monitor		X		X		X
3.2.2.4	KVM Switch		X		X		X
3.2.2.5	Ethernet Switch / Hub		X		X		X
3.2.2.6	Timeserver		X		X		X
3.2.2.7	Signal Entry Panel		X		X		X
3.2.2.8	ASIM and VPN Hardware		X	X			
3.2.3	Electrical Interfaces (External)		X				
3.2.3.1	Prime Power		X			X	X
3.2.3.2	IP 10BaseT/100BaseTX		X		X		X
3.2.3.3	100BaseFX		X		X		X
3.2.3.4	Console Ports		X		X		X
3.2.4	Electrical Interfaces (Internal) – TBS	X					
3.2.5	Packaging/Transit Cases and Monitor Kits		X				X
3.2.5.1	Weight					X	
3.2.5.2	Storage Space		X				
3.2.6	Cables and Accessories				X		X
3.2.7	Marking & Labeling		X				X
3.2.8	Reliability			X			
3.2.9	Maintainability			X			
3.2.10	Environnemental Conditions	X					
3.2.10.1	Temperature / Relative Humidity					X	
3.2.10.2	Altitude			X			
3.2.10.3	Sand and Dust			X			
3.2.10.4	Shock					X	

Table 4 - Verification Cross Reference Matrix

Paragraph	Title	Verification Method					
			PQT				
		N/R	Inspect	Analysis	Demo	Test	ATP
3.2.10.5	Vibration					X	
3.3	Design and Construction	X					
3.3.1	Materials Parts and Processes			X			
3.3.2	Safety	X					
3.3.2.1	Electrical Safety			X		X	
3.3.2.2	Mechanical Safety		X				
3.4	Logistics			X			

5.0 PREPARATION FOR DELIVERY

Each module is packaged for shipment and the package marked in accordance with the requirements of the contract under which the module is ordered.

6.0 BASELINE CONFIGURATION

6.1 Equipment

To be completed by NCC-D Heavy contractor.

Table 5 - Components

Device	Manufacturer	Part Number	Description	Quantity

6.2 Elevation Drawings

To be completed by NCC-D Heavy contractor.

Figure 4 - Front Elevation Drawing

To be completed by NCC-D Heavy ontractor

Figure 5 - Rear Elevation Drawing

6.3 Cable Diagrams

To be completed by NCC-D Heavy contractor.

Table 6 - Cables

Wire Number	Part Number	Manufacturer	Description

6.4 Interconnection Diagram

To be completed by NCC-D Heavy contractor.